*Change Management Policy*

Table of Contents

[Purpose 1](#_Toc3902690)

[Scope 1](#_Toc3902691)

[Policy 1](#_Toc3902692)

[Authorization and Review 1](#_Toc3902693)

[Change Procedures 2](#_Toc3902694)

[Change Documentation 2](#_Toc3902695)

[Recording Changes 2](#_Toc3902696)

[Change Testing 3](#_Toc3902697)

[Violations 3](#_Toc3902698)

[Definitions 3](#_Toc3902699)

[References 4](#_Toc3902700)

[Related Documents 4](#_Toc3902701)

[Approval and Ownership 4](#_Toc3902702)

[Revision History 5](#_Toc3902703)

Purpose

This policy defines the requirements for managing changes to any CompanyX (the “Company”) Information system.

Scope

This policy applies to all information security analysts and system Managers responsible for the maintenance of CompanyX Information systems.

Policy

### ****Authorization and Review****

**Production Operating System Changes** - Extensions, modifications, or replacements to production operating system software must be made only if the written approval of the manager of the Information Security Department has been received in advance.

**Change Approval** – All changes to CompanyX information systems equipment must be authorized by the Information Security Manager.

**Security Considerations For Production System Changes** - Prior to cut-over, every non-emergency change to production systems must be shown to be consistent with the information security architecture and approved by management as part of the formal change control process.

### ****Change Procedures****

**Change Control Procedure** - All Information systems used for production processing at CompanyX must employ a formal change control procedure to authorize all significant changes to software, hardware, communications networks, and related procedures.

**Production Change Personnel** - CompanyX production data and production computer programs must be changed only by authorized people according to established procedures.

**Systems Administrators Install/Update Server Software** - Only authorized Systems Administrators are permitted to install and/or update software on CompanyX servers.

**Back-Off Procedures** - Adequate back-off procedures, which permit information processing activities to quickly and expediently revert to conditions in effect prior to the most recent change in software, must be developed for all changes to production systems software and production application software.

**Production Information System Change Implementation** - All non-emergency production information systems changes must be communicated to affected parties at least two weeks prior to the change. The cut-over for all non-emergency changes must be held until the first weekend of each month.

**Vendor-Provided Systems Software Installation** - Prior to being installed, new or different versions of the operating system and related systems software for multi-user production computers must go through the established CompanyX change control process.

### ****Change Documentation****

**Change Documentation - Customer Impact** - Change control procedures for all changes to CompanyX system components must include the documentation of the estimated customer impact of each change.

**Change Control Documentation** - Production application change control documentation must be maintained so that management can readily determine exactly what changed and allow any and all prior versions of production applications to be readily recreated and pressed into service if necessary.

**Change Log On Every Server** - Every CompanyX server must have a change log which details changes to both hardware and software. At a minimum, this log must indicate the date of the change, the Systems Administrator making the change, the server component changed, and an explanation and/or justification for each change.

**Change Log Access** - System access controls must additionally be defined so that only authorized persons can make changes to production applications and/or change control records.

**Production Systems Change Documentation** - Documentation reflecting all significant changes to production Information systems at CompanyX must be prepared within a week from the time that a change took place. This documentation must reflect the proposed change, management approval, and the way in which the change was performed, who tested the changes, who cut-over to the changes, and who authorized the changes.

### ****Recording Changes****

**Change Logging** - The details of all changes to CompanyX information processing operating system software must be logged.

**Change Log Contents** –The Change Management Log must at least contain the:

* Date of submission
* Date of change
* Owner and custodian contact information
* Nature of the change
* Individual Performing the change
* Indication of success or failure

### Change Testing

**Post Change Testing** - All changes must be tested before they are approved on CompanyX production Information systems. This must include, but not limited to the validation of all input to prevent cross-site scripting, injection flaws, and malicious file execution, proper error handling, secure cryptographic storage, secure communications, and proper role-based access control.

**Change Testing - Operational Functionality** - Prior to release to production all changes must be tested for operational functionality.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. CompanyX reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. CompanyX does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, CompanyX reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or Third-Party who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

**Change** - Any modification to the information processing infrastructure that is a result of:

* An implementation of new functionality.
* An interruption of service.
* A repair of existing functionality.
* A removal of existing functionality.

**Change Management** - The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

**Custodian** - Guardian or caretaker of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

**Emergency Change** - When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

**Owner** - The manager or agent responsible for the function, which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

**Third-Party –** Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

**Scheduled Change** – A modification to the information processing infrastructure where formal notification was submitted, reviewed, and approved in advance of the change being made.

**Unscheduled Change** – A modification to the information processing infrastructure where formal notification was not submitted, reviewed, and approved in advance of the change being made. Unscheduled changes may be implemented to maintain system integrity and security in a timely manner to prevent an emergency situation.

**User -** Any CompanyX employee or Third-Party who has been authorized to access any CompanyX electronic information resource.

References

ISO/IEC 27002 – 12.1.2 Change management

NIST: CM-3 Configuration Change Control

PCI-DSS: 6.4 Change Control Processes

US-CSF PR.IP-3: Configuration change control processes are in place

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |